National Infrastructure Protection Center
CyberNotes

Issue #2002-13 *July 1, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between June 13 and June 28, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
4D Inc.[1]	Windows 98/NT 4.0/2000, MacOS 8.6/9.0/ 9.0.4/ 9.1/ 9.2/ 9.2.1/ 9.2.2	WebServer 6.7.3	A buffer overflow vulnerability exits due to insufficient bounds checking of HTTP requests, which could let a remote malicious user cause a Denial or Service or execute arbitrary code.	No workaround or patch available at time of publishing.	WebServer HTTP Request Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[1] Bugtraq, June 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Adobe[2]	Unix	Acrobat Reader (UNIX) 4.05	A vulnerability exists because temporary files are created insecurely when a PDF document is opened or printed, which could let a malicious user overwrite sensitive data.	Upgrade to 5.05 available at: http://www.adobe.com	Acrobat Reader Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites.
American Power Conversion [3]	Windows 95/98	Power Chute Plus 5.0.2	A vulnerability exists because during installation the Files\Pwrchute folder is shared with world writable permissions without user notification, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PowerChute Plus Insecure Shared Folder Permission	Medium	Bug discussed in newsgroups and websites.
AnalogX[4]	Multiple	Simple Server: Shout 1.0	A buffer overflow vulnerability exists when a malformed request is submitted, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://www.analogx.com/files/ssshouti.exe	SimpleServer Shout Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Apache Software Foundation [5]	Windows 2000	Tomcat 4.0.3	A vulnerability exists when a specially-crafted URL request is made for a non-existent resource, which could let a remote malicious user obtain sensitive information.	jakarta-tomcat-4.1.3.exe http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/v4.1.3-beta/bin/jakarta-tomcat-4.1.3.exe jakarta-tomcat-4.1.3.tar.gz http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/v4.1.3-beta/bin/jakarta-tomcat-4.1.3.tar.gz	Tomcat Web Root Path Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Apache Software Foundation [6]	Windows 2000	Tomcat 4.0.3	A remote Denial of Service vulnerability exists when a malicious user makes numerous malformed requests that contain a large number of null characters.	jakarta-tomcat-4.1.3.exe http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/v4.1.3-beta/bin/jakarta-tomcat-4.1.3.exe jakarta-tomcat-4.1.3.tar.gz http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/v4.1.3-beta/bin/jakarta-tomcat-4.1.3.tar.gz	Apache Tomcat Null Character Malformed Request Denial Of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[2] Securiteam, June 21, 2002.
[3] Bugtraq, June 20, 2002.
[4] Foundstone Labs, FS-062502-22-AXSH, June 25, 2002.
[5] KPMG-2002024, June 19, 2002.
[6] KPMG-2002025, June 20, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BasiliX[7]	Multiple	Webmail 1.10	Multiple vulnerabilities exist: a vulnerability exists due to a flaw in permissions on the /tmp/BasiliX directory, which could let a malicious user obtain sensitive information; a vulnerability exists because the attachment capability in Compose Mail can be fooled into treating any file on the web server as the uploaded file, which could let a malicious user obtain sensitive information; a vulnerability exists because user supplied input to a SQL query is not adequately filtered, which could let a malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists in SQL queries, which could let a malicious user execute arbitrary JavaScript.	No workaround or patch available at time of publishing.	Webmail Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
BEA Systems[8]	Windows 95/98/NT 4.0/2000, Unix	WebLogic Express 5.1, 5.1 SP1-6, WebLogic Server 5.1, 5.1 SP1-6	A vulnerability exists due to an anomaly in the pattern matching code, which could let a remote malicious user bypass the authorization (ACL) mechanisms and obtain unauthorized access.	Patch available at: ftp://ftpna.bea.com/pub/releases/patches/SecurityBEA00-0600.zip	WebLogic Access Controls Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Borland/ Inprise[9]	Unix	Interbase 6.0	Two vulnerabilities exist: a buffer overflow vulnerability exists in the 'gds_lock_mgr' root program, which could let a malicious user execute arbitrary code as root; and a buffer overflow vulnerability exists in the 'gds_drop' program, which could let a malicious user potentially execute arbitrary code.	No workaround or patch available at time of publishing.	Interbase GDS_Lock_ MGR & GDS_Drop Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Caldera Systems[10]	Unix	OpenUnix 8.0, UnixWare 7.1.1	A vulnerability exists in 'ppptalk,' which could let a malicious user obtain root privileges.	**UnixWare:** Ftp://ftp.caldera.com/pub/updates/UnixWare/CSSA-2001-SCO.27/erg711697a.Z **OpenUnix:** Ftp://ftp.caldera.com/pub/updates/OpenUNIX/CSSA-2002-SCO.27/erg712071.pkg.Z	UnixWare / Open UNIX ppptalk Privilege Escalation	**High**	Bug discussed in newsgroups and websites.

[7] Bugtraq, June 18, 2002.
[8] BEA Systems, Inc. Security Advisory, BEA00-06.00, June 24, 2002.
[9] Bugtraq, June 18, 2002.
[10] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.27, June 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Caucho Technology [11]	Windows 2000	Resin 2.0, 2.1.1, 2.1.2	A Directory Traversal vulnerability exists in the 'view_source.jsp' sample script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Resin Server 'view_source' Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Caucho Technology [12]	Windows 2000	Resin 2.1.1	A Denial of Service vulnerability exists when a malicious user tries to access non-existent resources if large variables are defined in the request.	Upgrade available at: http://www.caucho.com/download/resin-2.1.2.zip	Resin Server Denial of Service	Low	Bug discussed in newsgroups and websites.
Caucho Technology [13]	Windows 2000	Resin 2.1.1	A Denial of Service vulnerability exists in the DOS device "con" when a malicious user sends certain malformed URLs to the server.	Upgrade available at: http://www.caucho.com/download/	Resin Server DOS Device Denial of Service	Low	Bug discussed in newsgroups and websites.
Cisco Systems[14]	Multiple	All devices running Cisco IOS® Software supporting SSH; Catalyst 6000 switches running CatOS; PIX Firewall; Cisco 11000 Content Service Switch family	A Denial of Service vulnerability exists in the SSH implementation due to the failure to properly process large SSH packets.	Upgrades available at: http://www.cisco.com/warp/public/707/SSH-scanning.shtml#Software	Cisco SSH Denial of Service	Low	Bug discussed in newsgroups and websites.
Cisco Systems[15]	Multiple	IOS 11.3 XA, 11.3 T, 11.3 NA, 12.0 XR, 12.0 T, 12.0 SC, 12.0, 12.1T, 12.1 EC, 12.1 CX, 12.1, 12.2 XF, 12.2 T, 12.2 BC, 12.2	Two vulnerabilities exist: a vulnerability exists which affects Cisco uBR7200 and uBR7100 series routers due to a defect, which could allow arbitrary configuration files to be accepted by the network; and a vulnerability exists that involves cable modems not manufactured by Cisco because unauthorized configuration can be downloaded to the cable modem.	Patches are available for some versions of IOS. Cisco customers should contact their normal upgrade channels.	Cisco Cable Modem Termination System Authentication Bypass	Medium	Bug discussed in newsgroups and websites.

[11] Bugtraq, June 24, 2002.
[12] KPMG-2002021, June 17, 2002.
[13] KPMG-2002022, June 17, 2002.
[14] Security Advisory, June 27, 2002.
[15] Cisco Security Advisory, June 17, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[16]	Multiple	ONS 15454 Optical Transport Platform 3.1.0, 3.2.0	A remote Denial of Service vulnerability exists if an IP packet that contains non-zero Type of Service (TOS) bits in the header is sent by a malicious user to the Timing Control Card (TCC) LAN interface.	Upgrade available at: http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/r33docs/sftuprgd/index.htm.	ONS 15454 Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Cisco Systems[17]	Windows NT 4.0/2000	Secure ACS for Windows NT 3.0, 3.0.1	A Cross-Site scripting vulnerability exists in the web server component because the "action" argument that the 'setup.exe' handler uses does not properly validate user input, which could let a malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	Cisco Secure ACS Cross-site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco Systems[18]	MacOS X, Unix	VPN Client 3.5.1 for Solaris, 3.5.1 for Mac OS X, 3.5.1 for Linux	A buffer overflow vulnerability exists due to insufficient bounds checking in user-supplied arguments in the vpnclient command, which could let a malicious user obtain root access.	This has been resolved in version 3.5.2 available at: http://www.cisco.com/public/sw-center/	VPN Client Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
ComCity Corporation[19]	Windows 95/98/ME/ NT 4.0/2000, XP	SalesCart Pro 1.0, 1.5, 3.0, SalesCart-STD 1.2, 2.0	A security vulnerability exists because customer information is not properly secured, which could let a remote malicious user obtain sensitive information.	ComCity has suggested reading the "Getting Started" section of the manual, specifically on page 35 of the SalesCart 2.0 manual, or page 72 of the SalesCart PRO manual, and following the configuration instructions to resolve this issue.	SalesCart Customer Database Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
DEC fingerD[20]	Multiple	DEC fingerD 0.7	A format string vulnerability exists due to the unsafe use of syslog() to log externally supplied data, which could let a remote malicious user execute arbitrary instructions.	No workaround or patch available at time of publishing.	DECFingerD Format String	**High**	Bug discussed in newsgroups and websites.
Deep Metrix[21]	Windows	LiveStats 6.2	A vulnerability exists because HTML tags are not properly filtered when generating reports, which could let a malicious user execute HTML or script code.	No workaround or patch available at time of publishing.	LiveStats Script Injection	**High**	Bug discussed in newsgroups and websites.

[16] Cisco Security Advisory, June 19, 2002.
[17] sMax. Security Advisory, June 14, 2002.
[18] Cisco Security Advisory, June 19, 2002.
[19] Securiteam, June 22, 2002.
[20] Bugtraq, June 25, 2002.
[21] Securiteam, June 20, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Delta Scripts[22]	Multiple	PHP Classifieds 6.0.5	A Cross-Site Scripting vulnerability exists, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	PHP Classifieds Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
DPGS[23]	Multiple	Duma Photo Gallery System 0.99.4	A vulnerability exists because form field input is not properly validated, which could let a remote malicious user obtain sensitive information and overwrite files.	This software is no longer being maintained. It is not likely that the vendor will release a fix which address this issue.	DPGS Form Field Input Validation	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Game Cheats[24]	Windows	Advanced Web Server Professional 1.0.3 0000	A remote Denial of Service vulnerability exists when a malicious user makes a large number of invalid HTTP requests to the web server.	No workaround or patch available at time of publishing.	Advanced Web Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
GOST[25]	Multiple	34.19-2001 Standard Implementation	Vulnerabilities exists because it is possible to create a "universal signature" without the knowledge of the private key and a weak signature may be also be created, which could compromise private key data.	No workaround or patch available at time of publishing.	34.19-2001 Standard Implementation Key Data Compromise	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Systems[26]	Unix	CIFS/9000 Server A.01.06, A.01.05	A vulnerability exists in the /opt/cifsclient/bin/cifslogin utility due to improper bounds checking of user input, which could let a malicious user execute arbitrary code and obtain elevated privileges.	Upgrade to A.01.06, and then install patch available at: http://itrc.hp.com PHNE_24164	CIFSLogin Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
ht://Dig Group[27]	Unix	ht://Dig 3.1.5, 3.1.6, 3.2.0	A Cross-Site Scripting vulnerability exists due to insufficient santization of user supplied input, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	ht://Dig Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Hugo Cisneiros[28]	Multiple	phpSquid Pass 0.11	A vulnerability exists due to improper use of the 'ereg' PHP function, which could let a malicious user change another user's password and username.	Upgrade available at: http://prdownloads.sourceforge.net/phpsquidpass/phpsquidpass-0.2.tar.gz?download	PHPSquidPass Unauthorized User Deletion	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[22] Bugtraq, June 14, 2002.
[23] Securiteam, June 24, 2002.
[24] Bugtraq, June 21, 2002.
[25] Bugtraq, June 20, 2002.
[26] Securiteam, June 24, 2002.
[27] SecurityFocus, June 24, 2002.
[28] Bugtraq, June 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Imatix[29]	Windows 98/ME	Xitami for Windows 2.5 b5, 2.5 b4	A number of vulnerabilities exist in the Xitami 2.5 Beta GSL Templates due to inadequate checking of user input, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Xitami GSL Template	**High**	Bug discussed in newsgroups and websites.
Irssi[30]	Unix	Irssi 0.8.4	A remote Denial of Service vulnerability exists when a malicious user attempts to join a channel that has an overly long topic description.	Upgrade available at: http://www.irssi.org/?page=download	IRSSI Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Lumigent[31]	Windows	Log Explorer 3.0 1	Several vulnerabilities exist: a buffer overflow vulnerability exists in the 'xp_logattach.dll,' which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'xp_logattach_setport' stored procedure, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'xp_logattach' stored procedure, which could let a malicious user execute arbitrary code.	**Workaround:** The vendor suggests granting execute permissions of stored procedures to trusted users only. This issue will be fixed the next scheduled maintenance release, available in two to three weeks.	Log Explorer XP_LogAttach _StartProf, XP_LogAttach _SetPort & XP_LogAttach Buffer Overflows	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits has been published.
Mandrake Soft[32]	Unix	Linux Mandrake 8.2	A vulnerability exists in msec because default security settings leave users' home directories world readable, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Mandrake 8.2 Msec Insecure Default Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
MetaLinks[33]	Multiple	MetaCart2. sql	A security vulnerability exists because the user database is stored without access prevention, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	MetaCart2. SQL Database Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Mewsoft[34]	Multiple	NetAuction 3.0	A Cross-Site Scripting vulnerability exits because HTML code is not filtered from URI parameters, which could let a malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	NetAuction Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[29] Bugtraq, June 14, 2002.
[30] Bugtraq, June 19, 2002.
[31] Bugtraq, June 14, 2002.
[32] Bugtraq, June 17, 2002.
[33] Bugtraq, June 18, 2002.
[34] Bugtraq, June 14, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[35]	Windows 2000	Commerce Server 2000, 2000 SP1&2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists because the Profile Service contains an unchecked buffer in a section of code that handles certain types of API calls, which could let a malicious user cause a Denial of Service or execute arbitrary code and obtain complete control over the machine; a buffer overflow vulnerability exists in the Office Web Components (OWC) package because it contains an unchecked buffer, which could let a malicious user cause a Denial of Service or execute arbitrary code; a vulnerability exists because of a feature of the OWC package installer, which could let a remote malicious user execute arbitrary code; and a new variant of the ISAPI Filter vulnerability exists, which could let a malicious user obtain complete control over the system.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-033.asp	Commerce Server Multiple Vulnerabilities CVE Names: CAN-2002-0050, CAN-2002-0620, CAN-2002-0621, CAN-2002-0622, CAN-2002-0623	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Microsoft[36]	Windows 95/98/ME/ NT 4.0/2000, XP	Excel 2000, 2000 SR1, 2000 SP1, 2002, 2002 SP2; Office 2000; Office XP	Multiple vulnerabilities exist: a vulnerability exists due to the way inline macros that are associated with objects are handled, which could let a malicious user bypass the Macro Security Model and execute arbitrary macro code; a vulnerability exists due to the way macros are handled in workbooks when the workbook is opened via a hyperlink on a drawing shape, which could let a malicious user execute arbitrary macros; a vulnerability exists when an Excel workbook is opened that contains an XSL Stylesheet that has HTML scripting open, which could let a malicious user execute arbitrary HTML scripts; and a new variant of the Word Mail Merge vulnerability exists which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-031.asp	Excel Multiple Vulnerabilities CVE Names: CAN-2002-0616, CAN-2002-0617, CAN-2002-0618, CAN-2002-0619	**High**	Bug discussed in newsgroups and websites.

[35] Microsoft Security Bulletin, MS02-033, June 26, 2002.
[36] Microsoft Security Bulletin MS02-031, June 19, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[37]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.5, 6.0	A Denial of Service vulnerability exists due to the way certain types of Stylesheet input are handled.	No workaround or patch available at time of publishing.	Internet Explorer Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft[38]	Windows NT 4.0/2000	Microsoft JET 4.0, 4.0 SP1-SP5; SQL Server 2000, 2000 SP1&2,	A buffer overflow vulnerability exists in the 'OpenDataSource' function when combined with the MS Jet Engine, which could let a remote malicious user execute arbitrary instructions with the privileges of the SQL Server.	Microsoft advises affected users to obtain the latest version of Microsoft Jet Engine available at: http://www.microsoft.com/windows2000/downloads/recommended/q282010/default.asp?FinishURL=%2Fdownloads	SQL Server 2000 OpenData Source Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft[39]	Windows NT 4.0/2000	SQL Server 2000, SQL Server 2000 SP1&2	A buffer overflow vulnerability exists due to insufficient bounds checking of data supplied to the built-in PWDEncrypt() hashing function, which could let a malicious user execute arbitrary code and possibly create a Denial of Service.	No workaround or patch available at time of publishing.	SQL Server 2000 PWDEncrypt Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft[40]	Windows 95/98/ME/ NT 4.0/2000, XP	Windows Media Player XP, 6.4, 7.1	Several vulnerabilities exist: an information disclosure vulnerability exists due to the way the Windows Media Player handles certain types of licenses for secure media files when the media file is stored in the IE cache, which could let a malicious user execute arbitrary code; a privilege elevation vulnerability exists due to the way the Windows Media Device Manager Service handles requests to access local storage devices, which could let a malicious user obtain elevated privileges and take complete control over the machine; and a script execution vulnerability exists due to the way the Windows Media active playlist information is stored on the local system, which could let a malicious user execute arbitrary script code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-032.asp	Windows Media Player Multiple Vulnerabilities CVE Names: CAN-2002-0372, CAN-2002-0373, CAN-2002-0615	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[37] Securiteam, June 17, 2002.
[38] NGSSoftware Insight Security Research Advisory, NISR19062002, June 19, 2002.
[39] Securiteam, June 15, 2002.
[40] Microsoft Security Bulletin, MS02-032, June 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MIT[41]	Unix	CGIEmail 1.6	A vulnerability exists due to improper santization of user supplied values, which could let a malicious user use cgiemail as an open relay for e-mail.	No workaround or patch available at time of publishing.	CGIEmail Mail Relay	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
mod_ssl[42]	Multiple	mod_ssl 2.8.5-2.8.9	A buffer overflow vulnerability exists when handling certain types of long entries in an '.htacess' file, which could let a malicious user cause a Denial of Service or execute arbitrary code.	Upgrade available at: http://www.modssl.org/source/mod_ssl-2.8.10-1.3.26.tar.gz **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.1/common/008_mod_ssl.patch'	Mod_SSL HTAccess Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Multiple Vendors[43] ***HP issues patch for MPE/iX***[44]	**Windows 95/98/ME/ NT 4.0/2000, Unix**	***MPE/iX 4.0, 4.5, 5.0, 5.5, 6.0, 6.5, 7.0***	**Multiple vulnerabilities exist in several SNMP implementations in the process of decoding and interpreting SNMP trap messages. These vulnerabilities may cause Denial of Service conditions, service interruptions, and in some cases may allow a malicious user to gain access to the affected device. Specific impacts will vary from product to product.** ***Note: For more detailed information, see CERT® Advisory CA-2002-03, located at:*** **http://www.cert.org/advisories/ CA-2002-03.html.**	**Contact your vendor for patch or see CERT Advisory located at: http://www.cert.org/advisories/CA-2002-03.html** ***Patches available at: http://itrc.hp.com SNMGDL9A SNMGDM0A SNMGDM1A***	**Multiple Vendor SNMP Trap Handling** **CVE Name: CAN-2002-0012**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**

[41] Bugtraq, June 14, 2002.
[42] Bugtraq, June 24, 2002.
[43] CERT® Advisory CA-2002-03, February 12, 2002.
[44] Hewlett-Packard Company Security Bulletin, HPSBMP0206-015, June 17, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[45]	Windows 98, XP, Unix	Debian Linux 2.2 sparc, powerpc, IA-32, arm, alpha, 68k; Mandrake Soft Linux Mandrake 8.0, 8.0 ppc, 8.1, 8.1 ia64, 8.2; Microsoft Windows 98, 98SE, XP Home, XP Profes-sional; RedHat Linux 6.2 sparc, i386, alpha, Linux 7.0 sparc, i386, alpha, Linux 7.1 ia64, i386, alpha, Linux 7.2 ia64, i386, Linux 7.3 i386; SuSE Linux 6.4 ppc, i386, alpha, Linux 7.0 sparc, ppc, i386, alpha, 7.1 x86, 7.1 sparc, ppc, alpha, Linux 7.2 i386, Linux 7.3 sparc, 7.3 ppc, i386, Linux 8.0 i386	A Denial of Service vulnerability exists in the Internet Group Management Protocol (IGMP) report suppression mechanism when a malicious user sends a report addressed to the victim's Ethernet address.	No workaround or patch available at time of publishing.	Multiple Vendor IGMP Denial of Service	Low	Bug discussed in newsgroups and websites.

[45] Bugtraq, June 14, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[46, 47, 48]	Unix	FreeBSD 4.3, 4.3 – STABLE, 4.3 – RELENG, 4.3 - RELEASE 4.4, 4.4 – STABLE, 4.4 – RELENG, 4.5, 4.5 – STABLE, 4.5 – RELEASE, 4.6, 4.6 – RELEASE; ISC BIND 4.9, 4.9.3-4.9.7, 8.1, 8.1.1, 8.1.2, 8.2, 8.2.1-8.2.3; NetBSD NetBSD 1.4, 1.4 x86, SPARC, arm32, ALPHA, 1.4.1, 1.4.1 x86, SPARC, sh3, arm32, ALPHA, 1.4.2, 1.4.2 x86, SPARC, arm32, ALPHA, 1.4.3, 1.5, 1.5 x86, sh3, 1.5.1, 1.5.2; OpenBSD OpenBSD 2.7-3.1	A buffer overflow vulnerability exists in the DNS resolver code in libc, which could let a remote malicious user execute arbitrary code.	**FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:28/ **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/	Multiple Vendor libc DNS Resolver Code Buffer Overflow	High	Bug discussed in newsgroups and websites.

[46] Pine Internet Security Advisory, 20020601, June 25, 2002.
[47] NetBSD Security Advisory, 2002-006, June 27, 2002.
[48] FreeBSD Security Advisory, FreeBSD-SA-02:28, June 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[49, 50, 51, 52, 53, 54, 55, 56, 57]	Windows 95/98/NT 4.0/2000, XP, MacOS X 10.0-10.0.3, Unix	Apache Software Foundation Apache 1.0-1.0.3, 1.0.5, 1.1, 1.1.1, 1.2, 1.2.5, 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.9, 1.3.11-1.3.14, 1.3.11 win32-1.3.20 win32, 1.3.14 Mac, 1.3.17-1.3.20, 1.3.22-1.3.24, 1.3.22 win32-1.3.24 win32, 2.0. 2.0.28, 2.0.32, 2.0.35, 2.0.36	A vulnerability exists when invalid requests are coded with the 'Chunked Encoding' mechanism, which could let a remote malicious user cause a Denial of Service and in some cases execute arbitrary code. This can facilitate the further exploitation of vulnerabilities unrelated to Apache on the local system, potentially allowing the intruder root access. *Note: The impact of this vulnerability is dependent upon the software version and the hardware platform the server is running on.*	This issue is resolved in the Apache HTTP Server versions 1.3.26 and 2.0.39, available at: http://www.apache.org/dist/httpd/ **SuSE:** ftp://ftp.suse.com/pub/suse/pc/update/ **EnGarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ **RedHat:** ftp://updates.redhat.com/ **OpenPKG:** ftp://ftp.openpkg.org/release/1.0/UPD/apache-1.3.22-1.0.2.src.rpm **Debian:** http://security.debian.org/dists/stable/updates/main/ **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/ **Mandrake Linux:** http://www.mandrakesecure.net/en/ftp.php	Multiple Vendor Apache Chunked-Encoding Memory Corruption CVE Name: CAN-2002-0392	Low/**High** **(High if arbitrary code can be executed or if root access is obtained)**	Bug discussed in newsgroups and websites. Exploit scripts have been published. *Note: There is an Internet worm that uses the Chunked Encoding exploit.* Vulnerability has appeared in the press and other public media.

[49] CERT Advisory CA-2002-17, June 17, 2002.
[50] SuSE Security Announcement, SuSE-SA:2002:022, June 18, 2002.
[51] EnGarde Secure Linux Security Advisory, ESA-20020619-014, June 19, 2002.
[52] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:103-13, June 19, 2002.
[53] OpenPKG Security Advisory, OpenPKG-SA-2002.004, June 19, 2002.
[54] Debian Security Advisory DSA-131-2, June 19, 2002.
[55] Slackware Security Team, June 19, 2002.
[56] Trustix Secure Linux Security Advisory, TSLSA-2002-0056, June 20, 2002.
[57] Mandrake Linux Security Update Advisory, MDKSA-2002:039-2, June 22, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[58, 59, 60, 61, 62,63, 64, 65, 66, 67]	Unix	HP HP-UX Secure Shell A.03.10; OpenSSH 1.2.2, 1.2.3, 2.1, 2.1.1, 2.3, 2.5, 2.5.1, 2.5.2, 2.9, 2.9 p1&2, 2.9.9, 3.0, 3.0 p1, 3.0.1, 3.0.1 p1, 3.0.2, 3.0.2 p1, 3.1, 3.1 p1, 3.2, 3.2.2 p1, 3.2.3 p1, 3.3, 3.3 p1	Two vulnerabilities exist when the OpenSSH server is configured at compile-time to support the 'BSD_AUTH' or 'SKEY' authentication, which could let an unauthenticated remote malicious user execute arbitrary code with root privileges. The first vulnerability affects OpenSSH versions 2.9.9 through 3.3 that have the challenge response option enabled and use 'SKEY' or 'BSD_AUTH' authentication and the second vulnerability affects PAM modules which use the interactive keyboard authentication in OpenSSH versions 2.3.1p1 through 3.3, regardless of the challenge response option setting.	**OpenSSH:** ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/o/ **EnGarde:** http://ftp.engardelinux.org/pub/engarde/stable/updates/ **Mandrake:** ftp://ftp.nmt.edu/pub/linux/mandrake/updates/ ftp://mirrors.secsup.org/pub/linux/mandrake/Mandrake/updates/ **SuSE:** ftp://ftp.suse.com/pub/suse/ **OpenPKG:** ftp://ftp.openpkg.org/release/1.0/UPD/openssh-3.0.2p1-1.0.3.src.rpm **Trustix:** http://www.trustix.net/pub/Trustix/updates/ For more information on patches and workarounds see CERT® Advisory CA-2002-18 available at: http://www.cert.org/advisories/CA-2002-18.html	OpenSSH 'BSD_AUTH' or 'SKEY' Authentication	**High**	Bug discussed in newsgroups and websites. *Note: It has been reported that malicious individuals or organizations may be developing, or have developed functional exploit code.* Vulnerability has appeared in the press and other public media.
My Postcards[68]	Unix	My Postcards Platinum 5.0, 6.0	A vulnerability exists in the 'magiccard.cgi' script because some types of user input is not properly handled, which could let a remote malicious user disclose sensitive information.	No workaround or patch available at time of publishing.	MagicCard. 'magiccard.cgi' Sensitive Information	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[58] CERT® Advisory, CA-2002-18, June 25, 2002.
[59] Conectiva Linux Security Announcement, CLA-2002:500, June 25, 2002.
[60] EnGarde Secure Linux Security Advisory, ESA-20020625-015, June 25, 2002.
[61] SuSE Security Announcement, SuSE-SA:2002:023, June 25, 2002.
[62] OpenPKG Security Advisory, OpenPKG-SA-2002.005, June 26, 2002.
[63] NetBSD Security Advisory, 2002-005, June 27, 2002.
[64] Caldera International, Inc. Security Advisory, CSSA-2002-030.0, June 27, 2002.
[65] Debian Security Advisory, DSA-134-4, June 27, 2002.
[66] Mandrake Linux Security Update Advisory, MDKSA-2002:040, June 24, 2002.
[67] Trustix Secure Linux Security Advisory, 2002-0059, June 28, 2002.
[68] SecurityFocus, June 15, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NCipher Corporation[69]	Windows NT 4.0/2000	NForce, nShield	A vulnerability exists due to the interaction between the class com.ncipher.km.nfkm ConsoleCallBack and version 1.4.0 of the Java Runtime Environment on Windows, which could let a malicious user obtain smart card passphrases and unauthorized access to application keys.	Temporary workaround available at: http://www.ncipher.com/support/advisories/advisory4_java.html	ConsoleCall Back Class With JRE 1.4.0 Smart Card Passphrase Leak	Medium	Bug discussed in newsgroups and websites.
Netgear[70]	Multiple	RP114 Cable/DSL Web Safe Router Firmware 3.26	A vulnerability exists in the default configuration because access to administration tools is granted to systems, which could let a remote malicious user obtain full access to your router.	No workaround or patch available at time of publishing.	RP114 Administrative Access Via External Interface	**High**	Bug discussed in newsgroups and websites.
Noguska[71]	Unix	Nola 1.1.1, 1.1.2	A vulnerability exists in the Document Management Module because it allows php script to be uploaded, which could let a remote malicious user execute arbitrary files.	No workaround or patch available at time of publishing.	Nola Remote File Include	**High**	Bug discussed in newsgroups and websites.
Novell[72]	Multiple	Netware 6.0 SP1	A Denial of Service vulnerability exists in the DHCP (Dynamic Host Configuration Protocol) server when a malicious user sends a malformed DHCP request.	No workaround or patch available at time of publishing.	Netware DHCP Server Denial of Service	Low	Bug discussed in newsgroups and websites.
Novell[73]	Multiple	Netware 6.0 SP1	A remote Denial of Service vulnerability exists in NWFTPD when a malicious user sends format strings in the form of usernames.	No workaround or patch available at time of publishing.	Netware NWFTPD Format String Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Novell[74]	Multiple	Netware 6.0, 6.0 SP1	A Denial of Service vulnerability exists in the iManage feature when a malicious user supplies an unusually long string or arbitrary characters in the username field.	No workaround or patch available at time of publishing.	Netware iManage Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Os Commerce[75]	Multiple	Os Commerce 2.1	A vulnerability exists in 'include_once.php,' which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	OSCommerce Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

[69] nCipher[TM] Security Advisory No. 4, June 17, 2002.
[70] Bugtraq, June 17, 2002.
[71] Bugtraq, June 24, 2002.
[72] cqure.net Security Vulnerability Report, 20020604, June 25, 2002.
[73] cqure.net Security Vulnerability Report, 20020521, June 25, 2002.
[74] Cluestick Advisory #001, June 27, 2002.
[75] Bugtraq, June 16, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHP-Address[76]	Unix	PHP-Address 0.2e	A vulnerability exists regarding language handling, which could let a remote malicious user execute arbitrary PHP code.	Upgrade available at: http://www-user.tu-chemnitz.de/~chu/phpaddress/PHPAddress-0.2.f.tgz	PHP-Address Remote File Include	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
phpBB Group[77]	Multiple	phpBB 2.0.0, 2.0 RC1-4, 2.0.1	A vulnerability exists in the 'install.php' code when "allow_url_fopen" is set to "On" and "register_globals" is also set to "On" (in php.ini), which could let a remote malicious user execute arbitrary PHP code.	Unofficial Workaround (Bugtraq): Set "allow_url_fopen" to "Off" and "register_globals" to "Off." After you have completed the installation process remove or rename the install.php script.	PHPBB2 Install.PHP Remote File Include	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Pirch IRC[78]	Windows	Pirch IRC 98	A buffer overflow vulnerability exists when a long buffer is sent in either a channel or a private message due to the way malformed links are handled, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	Upgrade available at: www.pirch.com.	Pirch IRC Link Handling Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Rlaj[79]	Unix	WhoIS 1.0	A vulnerability exists because special symbols are not properly filtered for user supplied input, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Rlaj WhoIs Remote Shell Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Seunghyun Seo[80]	Multiple	MSN666 1.0, 1.0.1	A buffer overflow vulnerability exits because malformed MSN traffic may overflow a fixed width buffer, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	MSN666 Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
SGI[81]	Unix	IRIX 6.5-6.5.16	A vulnerability exists in the /usr/NetVis/etc/nveventd component of NetVisualyzer, which could let an unauthorized malicious user write to any file on the system. This could potentially lead to a root exploit.	SGI has announced that no patch will be released. Vulnerable users are advised to remove the suid bit from the 'nveventd' binary: # chmod u-s /usr/NetVis/etc/nveventd	SGI NetVisualyzer Arbitrary File Write CVE Name: CAN-2002-0631	Medium/ **High** **(High if root access can be obtained)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[76] Securiteam, June 18, 2002.
[77] Bugtraq, June 16, 2002.
[78] Bugtraq, June 21, 2002.
[79] sp00fed packet advisory #1, June 27, 2002.
[80] Gobbles Security Labs, June 13, 2002.
[81] SGI Security Advisory, 20020607-02-I, June 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SGI[82]	Unix	IRIX 6.2-6.5, 6.5.1-6.5.16, 6.5.1f-6.5.15f, 6.5.1m-6.5.15m	Several vulnerabilities exist: a vulnerability exists in popen() because arguments that are passed to the RPC are not sanitized, which could let a malicious user execute arbitrary commands with root privileges; and a vulnerability exists in the 'xfsmd' service due to a weak RPC authentication scheme, which could let a malicious user perform actions in the Unix system equivalent to gaining root user privileges.	SGI has stated that the product is being retired. No patches will be produced. Instructions are available for disabling the service at: http://www.sgi.com/support/security/advisories.html	IRIX rpc.xfsmd Remote Command Execution & Weak Authentication CVE Name: CAN-2002-0359	**High**	Bug discussed in newsgroups and websites. Exploit script has been published for the popen() vulnerability.
Summit Computer Networks[83]	Windows NT 4.0/2000	Lil'HTTP 2.1, 2.2	A Cross-Site Scripting vulnerability exists in the 'REPORT' function in the 'urlcount.cgi' script, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Lil' HTTP Server Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
Sun Micro-Systems, Inc.[84]	Unix	Solaris 8.0, 8.0 _x86	A vulnerability exists in 'dtscreen,' which could let a malicious user bypass authentication and obtain unauthorized access.	No workaround or patch available at time of publishing.	Solaris Screensaver Authentication Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-Systems, Inc.[85]	Unix	Solaris 9.0	A vulnerability exists when RPC is executed with excessively long command line arguments, which could let a malicious obtain elevated privileges.	No workaround or patch available at time of publishing.	Sun Solaris RCP Command Line Argument Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Valve Software[86]	Windows 95/98/ME/ NT 4.0, Unix	Half-Life 1.1.0.9, 1.1.0.8, 1.1.0.4 Windows, 1.1.0.4 Linux, 1.1.1.0, Dedicated Server 3.1 & previous, 3.1.3 x	A remote Denial of Service vulnerability exists when a malicious user creates a large number of new users on a specific server.	No workaround or patch available at time of publishing.	Half-Life Server New Player Flood Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Verity[87]	Multiple	Search97 2.1	A Cross-Site Scripting vulnerability exists due to the way search requests are processed, which could let a malicious user execute arbitrary script code.	Patch available at: https://customers.verity.com	Verity Search97 Error Page Cross Site Scripting	**High**	Bug discussed in newsgroups and websites.

[82] SGI Security Advisory, 20020605-01-I, June 20, 2002.
[83] Securiteam, June 28, 2002.
[84] Bugtraq, June 17, 2002.
[85] SecurityFocus, June 22, 2002.
[86] Bugtraq, June 20, 2002.
[87] Point Blank Security, June 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
WebScripts [88]	Multiple	WebBBS 4.0-4.2, 4.10-4.12, 4.20-4.22, 4.30-4.33, 5.0	A vulnerability exists because shell metacharacters are not properly filtered from CGI parameters, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	WebBBS Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Wolfram Research [89]	Windows, Unix	Web Mathematica Amateur 4.0, Professional 4.0	A Directory Traversal vulnerability exists in the MSP CGI program due to improper validation of user input, which could let a remote malicious user obtain sensitive information.	Customers are advised to contact Wolfram Research for update information. http://www.wolfram.com	Web Mathematica Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Working Resources Inc. [90]	Windows 95/98/ME/ NT 4.0/2000, X_P	BadBlue Enterprise Edition 1.7, Personal Edition 1.7	A vulnerability exists in the 'ext.dll' library because user input is not properly sanitized, which could let a malicious user execute arbitrary JavaScript.	No workaround or patch available at time of publishing.	BadBlue EXT.DLL Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
YaBB [91]	Unix	YaBB 1 Gold - SP 1	A Cross-Site Script vulnerability exists because URLs are not properly checked for script commands when error pages are generated, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	YaBB Gold Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Zeroboard [92]	Unix	Zeroboard 4.1 pl2	A vulnerability exists in the '_head.php' file because user input is not properly sanitized, which could let a remote malicious execute arbitrary code.	No workaround or patch available at time of publishing.	Zeroboard PHP Include File Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
ZyXEL [93]	Multiple	Prestige 642R	A Denial of Service vulnerability exists due to difficulties handling certain types of malformed packets.	No workaround or patch available at time of publishing.	Prestige 642R Malformed Packet Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

[88] Nerf gr0up: adv #7, June 18, 2002.
[89] Andrew Badr Security Advisory, June 17, 2002.
[90] SecurityFocus, June 23, 2002.
[91] AngryPacket Security Advisory, 0x0003, June 21, 2002.
[92] JCC Security Advisory, June 15, 2002.
[93] Bugtraq, June 17, 2002.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between June 13 and June 29, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 22 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
June 29, 2002	**Apache-chunked-scanner.zip**	**Apache Chunked Transfer vulnerability scanner for Windows.**
June 29, 2002	Ethereal-0.9.5.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
June 27, 2002	Telozarzo.c	Script which exploits the Telindus router 10xx and 11xx vulnerability.
June 24, 2002	Irx_xfsmd.c	Script which exploits the IRIX rpc.xfsmd Remote Command Execution vulnerability.
June 23, 2002	Apache-nosejob.zip	Script which exploits the FreeBSD, NetBSD, and OpenBSD Apache Chunked-Encoding Memory Corruption vulnerability.
June 22, 2002	Apache-nosejob.c	Script which exploits the FreeBSD, NetBSD, and OpenBSD Apache Chunked-Encoding Memory Corruption vulnerability.
June 22, 2002	Apache-smash.sh.gz	Denial of Service exploit for the Apache Chunked-Encoding Memory Corruption vulnerability.
June 22, 2002	Ddk-iis.c	Script which exploits the Microsoft ASP.NET Buffer Overflow vulnerability. Includes targets for IIS5 Chinese SP0, SP1, and SP2 and English SP2.
June 22, 2002	**Salescart-ex.c**	**Script which exploits the SalesCart Customer Database Disclosure vulnerability.**
June 20, 2002	Apachefun.tar.gz	Script which exploits the Apache Chunked-Encoding Memory Corruption vulnerability.
June 20, 2002	Apache-scalp.c	Script which exploits the Apache Chunked-Encoding Memory Corruption vulnerability.
June 20, 2002	Bed-0.3.zip	The Bruteforce Exploit Detector is a Perl script that remotely detects unknown buffer overflow vulnerabilities in FTP, SMTP, and POP daemons.
June 20, 2002	**Hl.zip**	**Exploit for the Half-Life Server New Player Flood Denial of Service vulnerability.**
June 20, 2002	Vpnkillient.c	Script which exploits the VPN Client Buffer Overflow vulnerability.
June 19, 2002	**Tracesex.pl**	**Perl script which exploits the TrACESroute Terminator Function Format String vulnerability.**
June 18, 2002	Icx2.c	Script which exploits the Icecast v1.3.11 and below remote root vulnerability for linux/x86.
June 18, 2002	**Interbase_gds_drop.pl**	**Exploit which exploits the Interbase GDS_Lock_MGR & GDS_Drop Buffer Overflow vulnerabilities.**

Date of Script (Reverse Chronological Order)	Script Name	Script Description
June 18, 2002	**Interbase_gds_l**	**Exploit which exploits the Interbase GDS_Lock_MGR & GDS_Drop Buffer Overflow vulnerabilities.**
June 18, 2002	Nmap-2.54beta36.tgz	A utility for port scanning large networks that supports Vanilla TCP connect() scanning, TCP SYN (half open) scanning, TCP FIN, Xmas, or NULL (stealth) scanning, TCP ftp proxy (bounce attack) scanning, SYN/FIN scanning using IP fragments (bypasses some packet filters), TCP ACK and Window scanning, UDP raw ICMP port unreachable scanning, ICMP scanning (ping-sweep), TCP Ping scanning, Direct (non portmapper) RPC scanning, Remote OS Identification by TCP/IP Fingerprinting, and Reverse-ident scanning.
June 18, 2002	**Ock_mgr.pl**	**Exploit which exploits the Interbase GDS_Lock_MGR & GDS_Drop Buffer Overflow vulnerabilities.**
June 18, 2002	**Webbbsexploit.pl**	**Perl script which exploits the WebBBS Remote Command Execution vulnerability.**
June 13, 2002	**Gobbles-own-msn666.c**	**Script which exploits the MSN666 Remote Buffer Overflow vulnerability.**

Trends

- **A warning has been issued by NIPC regarding a potential vulnerability in numerous versions of the open-source Apache Web Server Software. This vulnerability can allow remote access to the system and gives an intruder the ability to take control of the system and execute root level commands. NIPC considers this to be a significant threat due to the large installed base of Apache Servers, the potential for remote compromise, and the level of access granted by this vulnerability. For more information, see "Bugs, Holes, and Patches" table and NIPC Advisory 02-005, located at: http://www.nipc.gov/warnings/advisories/2002/02-005.1.htm**
- **BSD/Scalper.worm is an Internet Worm that spreads over Apache web servers on FreeBSD by using the Chunked Encoding exploit. For more information, see Virus Section. Also see the "Bugs, Holes, and Patches" table for more information regarding the vulnerability.**
- **Numerous exploit scripts exist which exploit the Apache Chunked-Encoding Memory Corruption vulnerability. For more information, see "Recent Exploit Scripts and Techniques" table.**
- **The CERT Coordination Center (CERT/CC) has issued an advisory on a new vulnerability in the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND). The vulnerability is in version 9 to 9.2 and not in versions 4 or 8. Exploitation of this vulnerability will cause vulnerable BIND server(s) to abort and shut down. For more information, see "Bugs, Holes, & Patches" table and NIPC Advisory 02-004.1, located at: http://www.nipc.gov/warnings/advisories/2002/02-004.htm.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included

information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Klez	Worm	Slight Increase	January 2002
2	W32/Magistr	File, Worm	Slight Increase	March 2001
3	W32/SirCam	Worm	Slight Decrease	July 2001
4	W32/Nimda	File, Worm	Slight Decrease	September 2001
5	Elkern	File Infector	Slight Decrease	October 2001
6	W32/BadTrans	Worm	Stable	April 2001
7	W32/Hybris	File, Worm	Slight Decrease	November 2000
8	VBS.VBSWG	Worm	New to Table	April 2002
9	JS Noclose.E	Trojan	New to Table	May 2002
10	W32/Yaha	Worm	New to Table	February 2002

Note: Virus reporting may be weeks behind the first discovery of infection. A total 206 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 389 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

BAT.Beckow.B@mm (Batch File Worm): This is a worm that sends itself to all addresses in the Microsoft Outlook Address Book. It also propagates through IRC. The worm attempts to copy itself to drive A, overwrite .reg, .vbs, .bat, ifk, .pif, and .lnk files, and delete files that are associated with several antivirus programs.

BAT_ERIS.A (Batch File Worm): This destructive, mass-mailing, batch file worm propagates via Microsoft Outlook. It sends e-mail messages with the following details:

- Subject: Hail Eris!
- Message Body: Hail Discordia! All Hail Discordia! Welcome to c0nfusion.
- Attachment: bat.eris.bat

The worm also deletes certain antivirus files, and on the system date, 23rd day of any month, it creates multiple folders in the root directory of the infected system's drive C:\.

BAT_EVERSAW.A (Aliases: VBS_ EVERSAW.A, IRC_ EVERSAW.A, I-Worm.Eversaw) (Batch File Worm): This batch file worm sends copies of itself to all addresses in the Microsoft Outlook address book. It sends an e-mail with the following details:

- Subject: "Ever saw an encrypted batch-worm? N0? then it's time!"
- Message Body: "Well, you don't have to execute the attachment (if you don't want to ;) ... hey, at least look at it! You can boast at your friends this evening at the strip: 'Hey comrades, today I saw an encrypted batch-worm!' ... Isn't that fascinating ?! "
- Attachment: BAT.FUCK.BAT

BAT_JERM.A (Aliases: I-Worm.Jerm, BAT/Jerm.Dropper) (Batch File): Upon execution, this batch file copies itself to a C:\Windows\UpgradeToWindowsXP.bat file and then overwrites malicious codes into the C:\mIRC\SCRIPT.INI file. IRC_JERM.A facilitates the sending of this batch file as an UpgradeToWindowsXP.bat to all Internet Relay Chat (IRC) users connected to the same IRC channel as the infected user. Next, it creates a XP folder, with read-only and hidden attributes, in the C:\ directory. In the same directory, it copies itself to a XP.BAT file, with normal attributes. The batch file worm also creates a registry file, C:\XPUpdate.reg, with normal attributes. XPUpdate.exe creates an entry as follows in the registry so that it executes upon Windows startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run PX "c:\\xp\\xp.bat

It carries a destructive payload by overwriting the contents of all C:\progra~1\mcafee\mcafee~1*.dat files with a copy of itself. It also creates a malicious Visual Basic Script (VBScript) file, C:\X.VBS with system and hidden attributes. VBS_JERM.A propagates copies of this batch file worm via e-mail. It uses Messaging Application Programming Interface (MAPI) commands to send an e-mail to all e-mail addresses listed in the infected user's Outlook Address Book. The details of the e-mail it sends are as follows:

- Subject: Upgrade to Windows XP
- Message Body: Good news from Microsoft. Click the attachment for your free Windows XP. Upgrade to Windows XP now."
- Attachment: UpgradeToWindowsXP.bat.

The VBScript file also adds this registry entry:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ CurrentVersion\Run XXP "c:\\xp\\xp.bat

This batch file worm also opens Internet Explorer and connects to the site: http://www.yahooka.com. It continuously pings www.hotmail.com thereby compromising Internet traffic.

IRC_JERM.A (IRC Script: This malware facilitates the propagation of the batch file worm, BAT_JERM.A, via Internet Relay Chat (IRC).

VBS_JERM.A (Visual Basic Script Worm): This component of BAT_JERM.A facilitates the mass-mailing routine of the batch file worm. It contains instructions to send an e-mail containing the following details to all recipients listed in the infected user's Outlook Address Book:

- Subject: Upgrade to Windows XP
- Message Body: Good news from Microsoft. Click the attachment for your free Windows XP. Upgrade to Windows XP now."
- Attachment: UpgradeToWindowsXP.bat

The VBS file also adds the registry entry:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run XXP "c:\\xp\\xp.bat

BAT_NOWE.A (Batch File): This destructive mass-mailing worm propagates via e-mail by sending copies of itself to all contacts in an infected user's Microsoft Outlook address book. It also propagates using mIRC, an Internet Relay Chat client. Upon execution, the batch file worm drops the following files in the root directory of drive C:\:

- C:\README.BAT
- C:\OWEN.VBS
- C:\IAmJustAWormWhoLovesWayne.VBS
- C:\IAmJustAWormWhoLovesCole.VBS

It drops these files into the Windows system directory, the desktop, and the startup folder:

- %SysDir%\WINI.BAT
- %WinDir%\Startm~1\Programs\StartUp\IAmJustAWormWhoLovesMills.VBS
- %Windir%\Desktop\I_LOVE_OWEN.BAT

This worm drops the following files into the current directory:

- VUDSP.BAT
- BeckhamOwen.REG
- IAmJustAWormWhoLovesBeckham.VBS
- IAmJustAWormWhoLovesFowler.VBS

It also creates the directory, C:\I_Am_Just_A_Simple_Worm_By_Galaxynet_IRC_#VX, where it drops the file, OWEN&BECKHAM.JPG.BAT. The worm then executes the dropped VBScript, OWEN.VBS, which applies MAPI to send copies of this batch file worm to all entries in the infected user's MS Outlook Address book. It sends the following e-mail message:

- Subject: "England Win WorldCup with Beckham" Message Body:
- Attachment: README.BAT

The worm also overwrites SCRIPT.INI file, if found in any of the following directories:

- C:\mirc32\script.ini

- C:\progra~1\mirc\script.ini
- C:\progra~1\mirc32\script.ini

The new SCRIPT.INI spreads the file, OWEN&BECKHAM.JPG.BAT, to any IRC user in the same channel as the infected user. The worm then overwrites .REG, .VBS, .BAT, .PIF, and .LNK files. It overwrites all .REG files with files that contain the following autostart entry, which is installed if any of the malware files are opened by an unsuspecting user or by an arbitrary application:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ CurrentVersion\Run ALERT = "%WinDir%\IAmOnlyJustAWormByBeckham.bat"

Next the worm overwrites all .VBS files in the directories with a code that executes the dropped file, IAmJustAWormWhoLovesOwen.VBS. It also overwrites all batch files (.BAT) in the same directories with its own copy. The worm replaces all .PIF files in the directories with a .PIF file that executes the dropped file, IAmJustAWormWhoLovesCampbell.VBS. It also overwrites all .LNK files in the mentioned directories with one that executes, ThisIsASimpleWorldCupWorm.VBS. It adds the following registry entry so that it is executed at every Windows startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ CurrentVersion\Run ksflt = "%WinDir%\IAmJustAWormWhoLovesRio.VBS"

The Windows configuration file, WIN.INI, is also overwritten by this worm. The new WIN.INI executes the Worm copy in the Windows system directory, WINI.BAT. SYSTEM.INI is also overwritten so that it executes VUDSP.BAT at startup. This worm attempts to delete Antiviral programs. This worm displays the following text before exiting:

- Beckham kick everyone asses! hehee! :P

IRC_NOWE.A (IRC Script): This IRC script malware is a component of the batch file worm, BAT_NOWE.A. It replaces the mIRC configuration file, SCRIPT.INI, to facilitate the worm's propagation using the Internet Relay Chat client.

VBS_NOWE.A (Visual Basic Script Worm): This VBScript malware is a component of the batch file worm, BAT_NOWE.A. It propagates the worm by sending the following e-mail message to all contacts in the infected user's Microsoft Outlook address book:

- Subject: "England Win WorldCup with Beckham"
- Attachment: README.BAT

BAT_WCUP.A (Alias: BAT.Wcup@mm) (Batch File Worm): This destructive batch file worm deletes antivirus software program files, and overwrites batch (.BAT) files in the Root and Windows directories, and overwrites the SYSTEM.INI and WIN.INI files of Windows. It propagates via Microsoft Outlook, and arrives in an e-mail message with the following:

- Subject: WorldCup News!
- Message Body: read me for more world cup news!
- Attachment: WorldCup.BAT

BAT.WCup.B@mm (Alias: Worm/BWG.F) (Batch File Virus): This is a script virus that attempts to distribute itself using Microsoft Outlook and mIRC. This threat may be received in e-mail in this format:

- Subject: Korean New Tactics To Defeat Germans
- Message: Tactics to win over the Germans!
- Attachment: germany_sucks.BAT

The worm creates a \Pro folder in the root of the hard disk and copies itself as C:\Pro\Korea.jpg.bat. It also attempts to modify the mIRC configuration file to send Korea.jpg.bat when you connect to IRC channels.

Benjamin (Aliases: Worm.Kazaa.Benjamin, Kazaa worm) (Internet Worm): The Benjamin worm uses KaZaa P2P (peer-to-peer) network to spread. The KaZaa network allows its participants to exchange files with each other, using the special client software. The worm is written in Borland Delphi. The worm's file is compressed with ASPack file compressor. When the worm's file is started, it shows a fake error message. Next it copies itself into Windows System directory as EXPLORER.SCR and creates two keys in the System Registry:

- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]"System-Service"="C:\\WINDOWS\\SYSTEM\\EXPLORER.SCR"

- [HKEY_LOCAL_MACHINE\Software\Microsoft] "syscod"="0065D7DB20008306B6A1"

This way the worm makes sure that it is always run when Windows is started. The worm spreads only from and to computers where KaZaa network clients are installed. The worm reads the settings of the KaZaa client from the System Registry, creates the directory named \Sys32\ in Windows Temp folder, and makes this directory visible to all clients of Kazaa network. The worm then fills this directory with its copies with various names that are taken from the list inside the worm's body. The list contains numerous titles of popular software, movies, games and music, and some commonly used search words. The worm spreads the following way: a KaZaa network user searches for any file (for example the file that has 'game' string in its file name) in the KaZaa network and finds it on the list of accessible files from an infected computer. He downloads this file and starts it, consequently infecting his own machine. The worm opens benjamin.xww.de Web-site to view an advertisement.

BSD/Scalper.worm (Internet Worm): This worm spreads over Apache web servers on FreeBSD by using the Chunked Encoding exploit. It first sends an ordinary request to the server. If it gets back a reply saying that the server is a vulnerable one "FreeBSD 4.5 x86 / Apache/1.3.20 (Unix)" or "FreeBSD 4.5 x86 / Apache/1.3.22-24 (Unix)," it will send the exploit. The worm appears to give a malicious user remote control abilities, including DDoS capability. There are two variants, 51,199 bytes and 51,626 bytes long.

PHP.Alf: This is a virus that infects files that have .php, .htm, and .html extensions. When PHP.Alf is executed, it first renames itself to Script.php. To accomplish this, it does the following:

- It renames itself to Dir.php
- It creates the C:\Php folder (if it does not exist)
- It moves itself to the C:\Php folder, still using the name Dir.php
- It moves itself back to the folder in which it originally ran, but using the name Script.php

Next, the virus searches for files that have the following extensions: .php, . htm, and .html. It opens each file that it finds and looks for the text string "Alf.php." If this text string is not found, the file will be infected. The infection is simply adding a reference to itself at the end of the file, so that the virus is executed each time that an infected file is opened. It appears that the search for the "Alf.php" string was meant to work as an infection marker, so that a file is infected only once. However, since the infection only means adding a reference to itself at the end, and not actually copying the virus into the file, files can be infected multiple times.

VBS_CHU.A (Alias: I-Worm.Chu) (Visual Basic Script Worm): This VBScript mass-mailer propagates via e-mail, sending out one of the following e-mail message:

- Subject: Upgrade MS Exchange or Update and upgrade MS Exchange
- Message Body: Run this attached file to upgrade MS Exchange.
- Attachment: MSXchange.vbs

It is capable of infecting other VBScript files (.VBS or .VBE).

VBS.Krim.B (Alias: VBS.Krim@mm) Visual Basic Script Worm): This is a variant of the VBS.Krim@mm worm that sends a component of itself to all contacts in the Microsoft Outlook Address Book. The mailed component is not capable of sending additional e-mail. If it is executed, it will attempt to format drive C. The e-mail would have the following characteristics:

- Subject: SMS for YOU by Valentina
- Attachment: Mirko.bat

VBS.Slip.B@mm (Visual Basic Script Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all contacts in the Microsoft Outlook Address Book. The e-mail message has the following characteristics:

- Subject: Actualizacion critica de Anti-virus
- Message: Actulizacion critica contra el virus KLEZ este es el ultimo parche para su desinfecion
- Attachment: The name of the attachment varies.

After the worm sends itself, it adds the value, scan_anti-virus ®, to the registry key

- HKEY_CURRENT_USER\Software

to avoid sending itself again the next time that it runs.

W32.Bajar.Worm.Int (Win32 Worm): W32.Bajar.Worm.Int copies and runs a .vbs file and attempts to mass-mail itself to all contacts in the Microsoft Outlook Address Book, but it fails to do so due to a programming bug.

W32.Gunsan (Win32 Worm): This is a worm that mass-mails itself and infects local drives and network shares. It opens a backdoor that allows a malicious user to control the computer using IRC.

W32/Higuy-A (Alias: I-Worm.Tettona) (Win32 Worm): This is an Internet worm with backdoor capabilities. It spreads via e-mail by sending itself to addresses found in the Windows address book. There is an English version and an Italian version. The virus has the following attached files: tattoo.exe, euro.exe, or tettona.exe. When run for the first time, the worm displays the fake error message: "VBRUN49.DLL not found! Unable to execute." Then it copies itself into the Windows folder as dllmgr32.exe. It sets the following registry entry so that it will be automatically run when Windows starts up.

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\DllManager = \dllmgr32.exe

W32.HLLW.Kazmor (Alias: W32/Kazmor.worm) (Win32 Worm): This is a worm that has backdoor Trojan capability, which allows a malicious user to gain control of the compromised computer. W32.HLLW.Kazmor spreads across a local network using shared drives. The worm also attempts to spread across KaZaa file-sharing networks. The worm disguises itself as movies, games, or porno-related programs, or as software files to trick KaZaa users into downloading the program and opening it. It is written in the Borland Delphi programming language.

W32.Hokilo.irc (IRC Worm): This is a threat that is designed to spread using mIRC. This threat does not contain a damaging payload. It is packaged in a Shell Scrap Object (.shs file) as an executable named Worldcup.exe. When the .shs file runs, it extracts and runs the embedded executable. The executable then creates the VBScript file C:\Hoko.vbs and runs it. The instructions in the VBScript file cause the script to find the mIRC installation folder and modify the Script.ini file to send a copy of the worm as C:\Worldcup.txt.shs. Next, the executable creates another file, C:\Hoko.bat, with instructions to display a short message within C:\Hoko.txt. One string in Hoko.txt is:

- IRC-Worm.Hoko by Kuasanagui / 13 Junio de 2002

W32.Kwbot.Worm (Win32 Worm): This worm has a backdoor Trojan capability, which allows a malicious user to gain control of the compromised computer. The worm can update itself by checking for newer versions over the Internet. It disguises itself as popular movie, game, or software files, and attempts to spread across KaZaa file-sharing networks by tricking KaZaa users into downloading the program and opening it.

W32.Sand.12300 (Win32 Virus): This is a Win32 file infector that infects files that have the .exe extension. Upon execution, it will infect one file in the same folder as the virus. It is written in Visual Basic. Upon execution, the virus extracts two files, Vir.exe, and H0st.exe. Vir.exe is the pure viral data, and H0st.exe is the original host program file. Once it has extracted these files, it executes both of them.

W32/Yaha-E (Aliases: W32.Yaha.F@mm, I-Worm.Lentin.f, W32/Lentin.E, Worm/Lentin.F, Yaha.E, W32/Yaha.g@MM) (Win32 Worm): This worm has been reported in the wild and has been reported from several different countries. It is a worm that spreads via e-mail. The worm has its own SMTP client software and uses either an SMTP server found by examining the Windows registry or one from a list contained within the worm itself. The e-mail sent by the worm is highly variable. The subject line of the e-mail is created using a combination of words and phrases. The From and Subject fields of the forwarded message are also variable. The attachment filename is made up of three parts: a name, and two extensions. The worm also creates a copy of itself in the Recycle folder with a name comprised of four random lower case characters. The path to this copy is then added to the following registry entry to ensure that the worm is run each time a program with an EXE extension is run:

- HKLM\exefile\shell\open\command\default

Two files are created in the Windows folder. One has a DLL extension and an eight-character name created from the same four characters used for the copy of the worm. This file contains a list of e-mail addresses found on the infected computer. The second file has the same name as the copy of the worm and a TXT extension. This is a simple text file containing the text "iNDian sNakes pResents yAha.E." The worm will attempt to disable security software. When the worm is first run, it will imitate a screen saver by repeatedly displaying the following messages on the screen in various colors:

- U r so cute today "!"!
- True Love never ends
- I like U very much!!!
- U r My Best Friend

A copy of the attachment in base64 encoded format is created in the folder C:\Windows\Temp with the filename "kitkat."

W32.Yaha.F@mm (Aliases: WORM_YAHA.E, Worm/Lentin.F, W32/Yaha.g@MM) (Win32 Worm): This worm has been reported in the wild. It is a mass-mailing worm that sends itself to all e-mail addresses that exist in the Microsoft Windows Address Book, the MSN Messenger List, the Yahoo Pager list, the ICQ list, and files that have extensions that contain the letters ht. The worm randomly chooses the subject and body of the e-mail message. The attachment will have a .bat, .pif or .scr file extension. Depending upon the name of the Recycled folder, the worm either copies itself to that folder or to the %Windows% folder. The name of the file that the worm creates consists of four randomly generated characters between "C" and "Y." It will also attempt to terminate AntiVirus and Firewall processes.

W97M_AYAM.A (Aliases: W97M/AYAM.A@mm, Macro.Office.Melissa-based, W97M.Maya.A) (Word 97 Macro Virus): This nondestructive Word macro virus does not infect, but rather propagates using Microsoft Outlook, spamming e-mail with the following details:

- Subject: Hi man, it's %Username%
- Message Body: This is the new net Story. It's great
- Attachment: Maya.doc
  *Where %Username% is the current infected user's name.

W97M.Dotor.A@mm (Word 97 Macro Virus): This is a macro virus that drops a Windows executable and disables Microsoft Word macro security. The macro virus infects when you open an infected document.

W97M.Twopey.A (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and templates. The properties of infected documents may be configured as follows:

- Author: OPEY A." 'GREETINGS TO ALL FILIPINO PROGRAMMERS !!!
- Title:OpeY 2k1 version - Philippines

WM97/Dest-J (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents and the global NORMAL.DOT template file. The virus does not have a payload.

Worm/Brazil (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, through the use of the Internet Rely Chat (IRC) network. The worm arrives through e-mail in the following format:

- Subject: Will Brazil Will Win Turkey? Read To Know The Tricks!
- Body: Trashing Turkey Tactics!! Fresh From Brazil Coach!!
- Attachment: lucio.vbs

If executed, the worm copies itself in the directory under which it is run using the filename "Cafu.BAT." It then copies itself the root directory (C:\) under the file names "lucio.vbs" and "marco.BAT." Once the spreading routine is finished, these files are then deleted. It will also create the directory "This_Is_Just_A_Simple_Worm_by_Galaxynet_IRC_#VX" in which the file "ronaldo.jpg.BAT" gets dropped. Additionally, the file "system.ini" file gets modified. So that it can spread through IRC, the following file gets modified, "script.ini." It will also try to delete various antivirus software applications, including "avp32.exe, antivir.vdf, tc.exe, scan.dat, tbav.dat, fpw32.dll, and various Norton applications." Worm/Brazil contains the following text:

- A Brazil Worm - To Trash Turkey In Next Match !!!
- Brazil shall win the World Cup 2002 !!

Worm/Mars (Alias: I-Worm.Mars) (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book. The worm arrives through e-mail in the following format:

- Subject: Congratulations for your site
- Body: Congratulations for your site. This is a good tool to improve it. Best Regards.
- Attachment: WebMakeFullInstall.exe

If executed, the worm copies itself in the \windows\%system% directory under the filenames "CFGWIZ32.exe," "DebugW32.exe," "DPLAYSVR.EXE_vbpe.exe," "DDHELP.EXE_vbpe.exe," "icwscrpt.exe_vbpe.exe," and "ODBCAD32.EXE_vbpe.exe." Additionally, the file "C:\WINDOWS\START MENU\PROGRAMS\STARTUP\START.VBS" also get created. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Debug"="C:\\WINDOWS\\SYSTEM\\DebugW32.exe

Worm/Wyrm (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, through the use of the Internet Rely Chat (IRC) network. The worm arrives through e-mail in the following format:

- Subject: Newest Windows Security Patch!
- Body: A new Loveletter version is making the rounds. This version is able to steal your Internet-access username and password. Here is the newest AntiVirus Patch against it.
- Attachment: bat.windows.bat

If executed, the worm copies itself in the directory under which it is run using the filename "bat.windows.bat." It then copies itself the root directory (C:\) under the file names "sig.sys." Once the spreading routine is finished, these files are then deleted. Additionally, the file "system.ini" file gets modified. So that it can spread through IRC, the following file gets modified, "script.ini." It will also try to delete various antivirus software applications, including avp32.exe, antivir.vdf, tc.exe, scan.dat, tbav.dat, fpw32.dll, and various Norton applications.

WORM_DOTOR.A (Alias: W32/Dotor-A, W97M.Dotor.A@mm) (Internet Worm): This mass-mailing worm arrives as the attachment, DOTOR.EXE, to an e-mail message. It sends an e-mail message with the following format to all addresses listed in the infected user's contact list:

- Subject: NewTool for Word Macro Virus
- Message Body: This tool allows you to protect you against unknown macro virus. Click on the attached file to run this freeware. Best Regards. Have a nice day.
- Attachment: DocTor.exe

WORM_FRETHEM.G (Alias: FRETHEM.G) (Internet Worm): This non-destructive, memory-resident variant of WORM_FRETHEM.A collects e-mail addresses from files found on the infected user's temporary Internet files folder and then sends it to one of the sites it connects to.

WORM_FRETHEM.I (Alias: FRETHEM.I) (Internet Worm): This nondestructive, memory-resident variant of WORM_FRETHEM.B propagates via e-mail. It arrives as an attachment to an e-mail message with the following details:

- Subject: Re: Your password!
- Attachments: Your password placed in password.txt, yourpassword.exe, password.txt

On systems with unpatched IE, the file attachments automatically execute when this e-mail message is previewed or opened in Microsoft Outlook and Outlook Express.

WORM_GLITCH.A (Alias: W32/Glitch@MM) (Internet Worm): This mass-mailing worm uses Microsoft Outlook to propagate, sending copies of itself as a file attachment. It sends e-mail messages to addresses taken from the Microsoft Outlook address book.

WORM_GUBED.A (Alias: W32.Gubed@mm) (Internet Worm): This mass-mailing worm propagates via Microsoft Outlook. It arrives as an attachment in an e-mail message with the following details:

- Subject: Congratulations for your site
- Message Body: Congratulations for your site. This is a good tool to improve it. Best Regards.
- Attachment: WebMakeFullInstall.exe

The worm copies itself as \%System%\DebugW32.exe, copies itself five times to both the \Windows and \Windows\System folder, and creates the Start.vbs file in the Startup folder. Start.vbs attempts to verwrite .vbs files that are in the My Documents folder and its subfolders.

WORM_MYPOWER.A (Aliases: MYPOWER, MYPOWER.A, W32.MyPower @mm) (Internet Worm): This destructive, mass-mailing worm arrives in an e-mail with predefined sets of subjects and message bodies. Its attachment usually carries a double extension .ZIP.SCR file and a ZIP file icon. It propagates via Microsoft Outlook by sending copies of itself to all users listed in the infected user's Global Address Book. It also deletes files, displays graphics, and plays sounds.

WORM_MYPOWER.B (Aliases: W32.MyPower.B@mm, MYPOWER.B, MYPOWER) (Internet Worm): This mass-mailing worm is a variant of WORM_MYPOWER.A and uses MAPI to send copies of itself to all users in the Windows Address Book (WAB). The subject, message body, and attachment are chosen from a predefined list.

WORM_SKREN.A (Alias: SKREN.A) (Internet Worm): This worm propagates via Microsoft Outlook by sending copies of itself to all users listed in the infected user's address book. It arrives in an e-mail with the subject line "Check Out This Cool Screensaver" and with the compressed attachment, "KellyOsbourne.com.gz." The worm copies itself to C:\KellyOsbourne.com. It also drops the file C:\Gz.exe, which is a compression utility that the worm uses to compress itself and create the file C:\KellyOsbourne.com.gz

WORM_ZOEK.D (Alias: I-Worm.Zoek.D) (Internet Worm): This worm is downloadable from a link to a Web site that arrives in an e-mail with the subject, "Maxima Screensaver." The worm takes the e-mail addresses from the Windows Address Book (WAB) and Outlook Mail Archives (DBX files). It also installs a backdoor malware, BKDR_BO2K, on the infected machine.

WORM_ZOEK.E (Aliases: W32.Zoek.E@mm, W32/Zoek.worm) (Internet Worm): This is a variant of the worm W32.Zoek@mm. It arrives as the attachment, "Screenmaxima.scr," and it attempts to disable Norton AntiVirus.

XM.Laroux.UB (Excel Macro Virus): This is a macro virus that spreads using Microsoft Excel. It infects under Excel 95, 97, 2000 and XP. This virus does nothing more than replicate.

X97M.Trevir (Alias: X97M.Sorry) (Excel 97 Macro Virus): This is a macro virus that infects Microsoft Excel workbooks. It uses virus code similar to that of W97M.Marker. This virus saves an infected workbook as the file XLStart.xls in the XLStart folder. It may password protect the workbook with the password "vir_ert."

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2002-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
APStrojan.sl	N/A	CyberNotes-2002-03
Arial	N/A	CyberNotes-2002-08
Backdoor.Anakha	**N/A**	**Current Issue**
Backdoor.AntiLam	N/A	CyberNotes-2002-12
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.GRM	**N/A**	**Current Issue**
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.Latinus	N/A	CyberNotes-2002-12
Backdoor.Mirab	**N/A**	**Current Issue**
Backdoor.NetControle	**N/A**	**Current Issue**
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	N/A	CyberNotes-2002-11
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.Sazo	**N/A**	**Current Issue**
Backdoor.Sparta	**N/A**	**Current Issue**
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Systsec	N/A	CyberNotes-2002-04
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	**N/A**	**Current Issue**
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/Osiris	N/A	CyberNotes-2002-06
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
BKDR_SMALLFEG.A	N/A	CyberNotes-2002-04
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
Dewin	N/A	CyberNotes-2002-08
DlDer	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Downloader-W	N/A	CyberNotes-2002-08
Fortnight	N/A	CyberNotes-2002-10
Hacktool.IPStealer	N/A	CyberNotes-2002-02

Trojan	Version	CyberNotes Issue #
Irc-Smallfeg	N/A	CyberNotes-2002-03
IRC-Smev	N/A	CyberNotes-2002-08
JS/NoClose	N/A	CyberNotes-2002-11
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11
RCServ	N/A	CyberNotes-2002-10
SecHole.Trojan	N/A	CyberNotes-2002-01
Swporta.Trojan	**N/A**	**Current Issue**
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/Zirko	N/A	CyberNotes-2002-10
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/DSS-A	N/A	CyberNotes-2002-12
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DSNX.A	N/A	CyberNotes-2002-03
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_WORTRON.10B	N/A	CyberNotes-2002-12
Trojan.Allclicks.A	**N/A**	**Current Issue**
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	**N/A**	**Current Issue**
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02

Trojan	Version	CyberNotes Issue #
VBS.Gascript	N/A	CyberNotes-2002-04
VBS_CHICK.B	N/A	CyberNotes-2002-07
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	**N/A**	**Current Issue**
W32.Libi	N/A	CyberNotes-2002-10
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Tendoolf	N/A	CyberNotes-2002-09
WbeCheck	N/A	CyberNotes-2002-09

Backdoor.Anakha (Aliases: Backdoor.Trojan, Trojan.Win32.Anakha.b, BackDoor-UY, Troj/Anaka-B): This is a backdoor Trojan horse that allows a malicious user to use Internet Relay Chat (IRC) to gain control of a computer. It also opens TCP/UDP ports to allow a malicious user to take control of the system. Backdoor.Anakha is written in the Microsoft Visual Basic programming language and is compressed with ASPack.

Backdoor.GRM (Aliases: Backdoor.Trojan, Backdoor.Galaxy, BackDoor-ZR): This is a backdoor Trojan that allows unauthorized remote access to an infected computer. The Trojan listens for connections on port 7614. It copies itself to \%System%\Grm.exe. If Backdoor.GRM is executed, it allows unauthorized remote access to an infected computer. Once connected to port 7614, the malicious user could perform actions such as:

- Opening and closing the CD-ROM drive
- Using Telnet to connect to another computer
- Moving or deleting files

Backdoor.GRM configures itself to run when you start Windows by adding the value, GRM %System%\Grm.exe, to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

Backdoor.Mirab: This Trojan allows a malicious user to remotely control an infected computer. It is written in the Borland Delphi programming language and compressed with UPX. By default, it uses port 4912 for direct control and port 6430 for file transfer. The messages that the Trojan displays and the name of the file that it drops may vary. The malicious user who creates this Trojan determines these. The Trojan repeatedly opens TCP/UDP ports. This may cause a degradation of computer performance. The malicious user who creates the Backdoor.Mirab server file, can add many functions. For example, it can be programmed to:

- Choose the ports that are used by the Trojan to communicate with the malicious user.
- Use different notification methods to send information to the malicious user about the compromised computer. For example, it attempts to open an HTTP connection to a Web server of the malicious user's choice, and post the victim's information to a script file on that Web server. The information may include:
  - Notification that the victim is online
  - The connection port
  - The upload/download port
  - The computer's system date and time

The Trojan also uses ICQ pager to send the compromised computer's information to the malicious user. If Backdoor.Mirab runs, it allows the malicious user to remotely take control over the compromised computer, and can include the ability to:

- Steal information from the host computer
- Take full control over the file system
- Upload to and download from the host computer

- Rename, delete, list, and run files of the malicious user's choice
- Delete folders
- Display messages
- View the screen
- Log keystrokes
- Shut down the host computer
- Perform annoying actions, such as: Change various desktop settings (wallpaper, resolution, etc.)
- Manipulate the mouse
- Close, hide, minimize, and maximize Windows
- Turn the monitor on and off

Backdoor.NetControle (Aliases: Backdoor.VB.o, Troj/Bdoor-VBO, Backdoor.Trojan): This is a Trojan horse that allows a malicious user to remotely control an infected computer. It is written in the Visual Basic programming language and can only run if the computer contains the Visual Basic runtime libraries. When this Trojan runs, it adds the value, Client <Trojan file name>, the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

The Trojan then opens a connection on TCP/UDP port 1772 to connect to the malicious user. This allows the malicious user to remotely take control of the compromised computer, and can include the ability to:

- Shut down/restart the compromised computer
- Open and close the CD-ROM drive tray
- Hide/show the taskbar
- Manipulate the mouse
- Beep

Backdoor.Sazo: This is a Trojan horse that connects to a malicious user's FTP site and downloads other components or updates for the Trojan. It can also send information from the computer back to the malicious user. The Backdoor also use of port 1218. It is written in Visual Basic and can only run if the computer contains the Visual Basic runtime libraries. When this Trojan runs, it does the following:

- It copies itself into the \Windows\System32 folder.
- It then adds the value, kernel .exe C:\Windows\System32\kernel.exe, to the registry key:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Services

Backdoor.Sparta: This is a Trojan horse that allows unauthorized access to the infected computer. This Trojan also attempts to remove several major brands of firewall and antivirus protection, including Norton AntiVirus.

Backdoor.Ultor: This is a backdoor Trojan that allows unauthorized access to an infected computer. The Trojan listens on either port 1111 or port 1234 for a connection. After a connection has been established, the malicious user will have full control of the infected computer.

Swporta.Trojan: This is a Trojan that attempts to modify the Web browser's home page. It requires various components in order to work. When the Trojan is executed, it changes these values: Start Page, and Startpagina, in the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\

to a HTML page on the local hard drive. In this way, the Trojan modifies the default Internet Explorer home page to the website predefined by the malicious user. Next it adds the subkey, SWCaller\SWCaller, under the registry key:

- HKEY_CURRENT_USER\Software

and sets its value to SWStartPage Yes. The Trojan may also add a value that refers to itself to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs each time when you start Windows. Some text files may be created by the Trojan. These files are named in the form of www.<some URL>.cxq. Most of the URLs relate to some adult Internet site in the Netherlands.

Trojan.Allclicks.A (Aliases: TrojanClicker.NetBuie.a, Trojan/Win32.Elitec, Trojan.NetBuie.A): This is a Trojan horse that comes disguised as an XBox emulator. The only purpose of this Trojan is to produce periodic hits on a specific Internet Web page. (At the time that this write-up was published, the Web site had been removed.) The XBox emulator in question is a fake emulator program produced by Linar Software/Studios.

Trojan.PSW.M2: This Trojan belongs to the family of Trojan horses that are capable of stealing various passwords. It has a program "configurer" that allows the malicious user to adjust server components. After restart, the Trojan copies itself over again in the %WinDir% directory, or in the directory %WinDir%System (depending on the given adjustments) and then registers itself in the system registry. It searches on a disk for the files containing passwords and also reads out the configuration of modem adjustments. It has an auto-updating function.

W32.Estrella: This is a Trojan horse that is designed to spread through floppy disks. This Trojan deletes some specific files on December 15th. It is written in Microsoft Visual Basic programming language. As part of its routine, W32.Estrella creates a copy of itself on a floppy disk as A:\Estrella.exe and has the standard Windows folder icon to deceive you. If A:\Estrella.exe (the Trojan) is then executed, it does the following:

- It adds the following values:
  - Win32G C:\%System%\Kernel32.com
  - Win32R C:\%Windows%\Server.com

to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

It adds the value:

- Win32G C:\%Windows%\COMMAND\Scandisk.com

to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

As a result of the three registry value additions, the Trojan runs when you start Windows. Next, it copies itself as:

- C:\%Windows%\Server.com
- C:\%System%\Kernel32.com
- C:\%Windows%\COMMAND\Scandisk.com